



BILLING CODE 3410-DM-P

DEPARTMENT OF AGRICULTURE

Office of the Secretary

[Docket No. FSIS-2011-0030]

Privacy Act of 1974; New System of Records

AGENCY: Food Safety and Inspection Service, USDA.

ACTION: Notice of proposed new system of records; request for comment.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the U.S. Department of Agriculture (USDA) proposes to establish a new system of records titled USDA/FSIS-03 Food Safety and Inspection Service (FSIS) Consumer Complaint Monitoring System (CCMS) II.

The mission of FSIS is to protect public health by ensuring that meat, poultry, and processed egg products are safe, wholesome, and accurately labeled. Thus, the Agency must detect food safety vulnerabilities as early and as specifically as possible so that the potential for harm can be promptly prevented, reduced, or eliminated. The CCMS II helps FSIS to effectively identify potentially unsafe meat, poultry, or processed egg products regulated by FSIS by recording, sorting, analyzing, and tracking consumer complaints regarding products'

potential adverse effects, and by tracking any subsequent analyses and investigations of those complaints.

DATES: Effective Date: [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]. If no comments are received, the proposal will become effective on above date. If comments are received, they will be considered and, where adopted, the document will be republished with changes.

ADDRESSES: You may submit comments, identified by docket number FSIS-2011-0030, by one of the following methods.

- Federal e-Rulemaking Portal: <http://www.regulations.gov>.
Follow the instructions for submitting comments.
- Mail: Director, Applied Epidemiology Division, Office of Public Health Science, Food Safety and Inspection Service, 1400 Independence Avenue, SW., Washington, DC 20250.
Fax: (202) 720-8213.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

- Docket: For access to the docket, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please

contact Dr. Karen Becker, Director, Applied Epidemiology Staff, Office of Public Health Systems, Food Safety and Inspection Service, Department of Agriculture, Washington, DC, 20024; telephone (202) 690-6045. For privacy questions, please contact Ravoyne Payton, Acting Chief Privacy Officer, Policy, E-Government and Fair Information Practices, Office of the Chief Information Officer, Department of Agriculture, Washington, DC, 20250; telephone (202) 720-8755.

SUPPLEMENTARY INFORMATION:

The Privacy Act of 1974, as amended (5 U.S.C. 552a), requires agencies to publish in the Federal Register a notice of new or revised systems of records maintained by the agency. A system of records contains information that is retrieved by an individual's name or other unique identifier. FSIS is proposing to establish a new Privacy Act system of records, entitled USDA/FSIS-03, FSIS Consumer Complaint Monitoring System II (CCMS II) , a relational database that collects information, retrieved by name or a unique identifying number assigned to an individual, to assist FSIS with trace-back or trace-forward investigations and characterization of foodborne hazards. The primary goal of the CCMS II electronic database is to support and augment FSIS analysts in their ability to identify consumer health risks associated with regulated products. The CCMS II

will assist FSIS to accomplish its safety mission by quickly and effectively identifying potentially unsafe meat, poultry, or processed egg products. More specifically, CCMS II helps FSIS to analyze, evaluate, and identify foodborne hazards in its regulated products; to assess the risk to human health; and to determine the appropriate response to known, emerging, or potential threats to the food supply or to the agriculture sector. Paper records printed from the electronic database are stored only in limited quantities and on rare occasions and are retrieved when needed as working copies. Such paper records are shredded upon termination of the need for a working copy.

Information gathered and entered into CCMS II supports investigations that can involve trace back to sources of foodborne illness outbreaks and tracing hazardous product forward to identify distribution and disposition. Among other activities, CCMS II data and investigations may support complaint-related verification of hazard analysis and critical control points in producing establishments, analysis of school lunch product manufacturing specifications associated with an outbreak involving a National School Lunch Program product, and recall coordination for products identified as being adulterated or unwholesome. If a complaint involves an incident that is determined to be non-routine, alerts will be provided to

management.

A complaint that is put into CCMS II can be initiated in any of the following ways: (1) calls from consumers or their representatives, or from representatives of State or local health departments and Federal agencies, including USDA's Agricultural Marketing Service (AMS) and Food and Nutrition Service (FNS), (2) electronic hand-off from the USDA's Meat and Poultry Hotline system, and (3) web forms submitted by consumers. Trained analysts review the complaint information. Once reviewed, the case is entered into the system directly or indirectly via a transfer from the Meat and Poultry Hotline System.

Epidemiologists in the FSIS Office of Public Health Science (OPHS) analyze the information in CCMS II to determine necessary further analyses, investigation, or processing. OPHS leads the management and investigation of all cases entered into the system. Technical and scientific support is provided to other program areas, as necessary.

Personal information about individuals collected in CCMS II includes first and last name, home or work address, telephone number or e-mail, and details of the complaint, which can include medical symptoms and medical treatment obtained. Specific information about food items eaten also is collected in

CCMS II. A unique case number is assigned to each complaint and provided to the individual making the report and can be used in lieu of or in addition to the personal information noted above for retrieving system information.

Under the Federal Meat Inspection Act (21 U.S.C. 601 et seq.), the Poultry Product Inspection Act (21 U.S.C. 451 et seq.), and the Egg Products Inspection Act (21 U.S.C. 1031 et seq.), FSIS is authorized to inspect and regulate the production of meat, poultry, and egg products and to prevent the sale and movement in commerce of adulterated or misbranded articles in order to fulfill its food safety mission. In addition, the Secretary of Agriculture is authorized to give high priority to enhancing the ability of FSIS "...to ensure the safety and wholesomeness of meat and poultry products;" to strengthen the ability of FSIS "to collaborate with relevant agencies within the Department of Agriculture and with other entities in the Federal Government, the States, and Indian tribes... through the sharing of information and technology;" and expanding the capacity of FSIS "to protect against the threat of bioterrorism" (21 U.S.C. 679c (a) (1) (3) and (4)).

In summary, all of these authorities allow FSIS to perform the functions of this system: to gather and maintain information related to foodborne hazards that will support investigations

aimed to trace back foodborne illness outbreaks to its sources and to identify potentially unsafe meat, poultry, or processed egg products from entering commerce; to collaborate with federal, State, local, and tribal public health partners in identifying potentially unsafe meat or poultry products; and to assess probable threats or risks to the food supply and devise an adequate response, to ultimately achieve its food safety mission.

Background

CCMS II system programs and use of resources comply with procedures for avoiding waste, fraud, abuse, or mismanagement; for obtaining, reporting, and using reliable and timely information for decision-making; and for appropriately identifying and managing program risks. To enable management and audit oversight, CCMS II includes management controls and performance measures for supported activities to ensure that decision-making is accurate, timely, complete, and effective.

There are no Privacy Act exemptions being made for this application. Consistent with USDA's public health mission, information stored in CCMS II may be shared with other USDA components, as well as with appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will take place only after USDA determines that the

receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

In accordance with 5 U.S.C. 552a(r), as implemented by Office of Management and Budget Circular A-130, FSIS has provided a report of this new system of records to: the Chairman, Committee on Homeland Security and Governmental Affairs, United States Senate; the Ranking Member, Committee on Homeland Security and Governmental Affairs, United States Senate; the Chairman, Committee on Oversight and Government Reform, House of Representatives; the Ranking Member, Committee on Oversight and Governmental Reform, House of Representatives; and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget.

Alfred V. Almanza
Acting Administrator.

USDA/FSIS-03

System of records name:

USDA/FSIS-03, FSIS Consumer Complaint Monitoring System
(CCMS) II

Security classification:

Unclassified

System location:

Records are maintained at the U.S. Department of Agriculture, 1400 Independence Avenue, SW., Washington, DC 20250, and at USDA's National Information Technology Center facility at 8930 Ward Parkway, Kansas City, Missouri, 64114.

Categories of individuals covered by the system:

Federal employees and private citizens involved in an FSIS investigation, including individuals who submit complaints; those who work in the food industry under FSIS' inspection, such as private citizens who operate or work at establishments; those who work for operations that may be subject to FSIS surveillance or enforcement, such as private citizens employed at retail operations that grind meat or poultry; members of volunteer organizations who prepare or have prepared food; and State, tribal, and local government employees responsible for food safety or public health.

Categories of records in the system:

This system contains information pertaining to investigations of consumer complaints to aid in identifying and tracking potential public health crises. This information includes personal information, such as first and last names, home or work address, telephone number or e-mail, and details concerning medical symptoms and care and cause of complaint. Each record is associated with an assigned case code to ease retrieval.

Authority for maintenance of the system:

- Poultry Products Inspection Act (21 U.S.C. 451 et seq.);
- Federal Meat Inspection Act (21 U.S.C. 601 et seq.); and
- Egg Products Inspection Act (21 U.S.C 1031 et seq.).

Responsible agency official for system:

Dr. David Goldman, Assistant Administrator, Office of Public Health Science (OPHS), Food Safety and Inspection Service(FSIS), U.S. Department of Agriculture, 1400 Independence Avenue, SW., Washington, DC 20250, Rm. 341-E JLW Bldg. Telephone (202) 720-2644.

Or Dr. Karen Becker, Director Applied Epidemiology Division, Office of Public Health Science, Food Safety and Inspection Service, U.S. Department of Agriculture, 1400 Independence Avenue, SW., Washington, DC 20250. Telephone (202) 690-6045; Fax:(202) 720-8213.

Purposes:

The records provided by and about individuals in this system are used by FSIS to sort, evaluate, and investigate possible adverse effects from FSIS-regulated products. The information also supports trace back to the source of foodborne illness outbreaks and tracing hazardous products forward to identify distribution and disposition. CCMS II data and associated processes help FSIS to analyze, evaluate, and identify foodborne hazards in products regulated by the Agency; to assess the risk to human health; and to determine the appropriate response to known, emerging, or potential threats to the food supply or to the agriculture sector.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, all or a portion of the records or information contained in this system may be disclosed outside USDA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. To the U.S. Department of Justice (DOJ) (including United States Attorney Offices) or other Federal agency conducting litigation, or in proceedings before any court, adjudicative or administrative body, when it is necessary for

the litigation, and one of the following is a party to the litigation or has an interest in the litigation:

- a. USDA or any component thereof;
- b. any employee of USDA in his/her official capacity;
- c. any employee of USDA in his/her individual capacity where DOJ or USDA has agreed to represent the employee; or
- d. the United States or any agency thereof, and USDA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which USDA collected the records.

2. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the written request of the individual to whom the record pertains.

3. To the National Archives and Records Administration (NARA) or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

4. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and

relevant to such audit or oversight function. This would include, but not be limited to the Comptroller General or any of his authorized representatives in the course of the performance of the duties of the Government Accountability Office, or USDA's Office of the Inspector General or any authorized representatives of that office.

5. To appropriate agencies, entities, and persons when:

a. USDA or FSIS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

b. USDA has determined that, as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by USDA or another agency or entity), or harm to the individual or individuals that rely upon the compromised information; and

c. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

6. To contractors and their agents, grantees, experts, consultants, and others performing or working on a

contract, service, grant, cooperative agreement, or other assignment for USDA, when necessary to accomplish an agency function related to this system of records. Individuals who provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to USDA officers and employees.

7. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

8. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or appropriate authority responsible for protecting public health, preventing or monitoring disease or illness outbreaks, or ensuring the safety of the food supply. This includes the Department of Health and Human Services and

its agencies, including the Centers for Disease Control and Prevention and the Food and Drug Administration, other Federal agencies, and State, tribal, and local health departments. Certain complaint-related information may be shared with the producing establishment for purposes of investigating the complaints. Except as stated, disclosure is made pursuant to requests under the Freedom of Information Act (FOIA).

Disclosure to consumer reporting agencies:

None

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored electronically in a dedicated virtual server or on paper in secure facilities in a locked drawer behind a locked door within USDA facilities. Electronically stored records, including backup records maintained on their own dedicated virtual server in a separate location, are stored on magnetic disc, tape, digital media, and CD-ROM. (Paper records are printed from electronic storage only in limited quantities and on rare occasions when needed as working copies. Such paper records are kept in secure facilities in a locked drawer behind a locked door within USDA

facilities, and immediately are shredded upon termination of the need for a working copy.) Security guards safeguard the buildings where the electronic and the working copies of records reside.

Retrievability:

Retrieval is generally performed using the case code (a sequentially assigned, system-generated code created at the time of initial contact) or other database fields, such as establishment number or type of complaint. A name can also be used to retrieve individual records; however, using the case code or other database fields reduces the need for retrieval by information that could identify an individual.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable USDA automated systems security and access policies. This includes protection behind firewalls, network protection against intrusion, and vulnerability scanning and protection. Only users with a business need are allowed access through the use of an encrypted password. Role-based access controls are used to restrict access to CCMS II, which is accessible via the FSIS Intranet. Furthermore, multiple levels of access exist, based on the user's system role and job function. Each time users

sign in to the application, the login credentials are checked against authorized system user role memberships to ensure the user's access privileges are restricted to assigned level-of-access roles. User activity is also monitored, logged, and audited. Additionally, all users are required to undergo USDA-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access. An access agreement describes prohibited activities, such as browsing.

Retention and disposal:

Records will be destroyed or maintained in accordance with the USDA's published records disposition schedules, as approved by NARA. A backup of the Master File is created at the end of the calendar year, and backup records are maintained in accordance with General Records Schedule Authority N1-462-07-01, Item 2. System inputs are maintained in accordance with General Records Schedule Authority GRS 20, Item 2(a) (4), while system outputs (reports) are maintained in accordance with General Records Schedule Authority GRS 20, Item 16.

System manager and address:

Dr. Karen Becker Director, Applied Epidemiology Staff, Office of Public Health Science, Food Safety and Inspection Service,

355 E Street SW PPIII, 9th Floor Office 9-232, Washington, DC 20024. Telephone (202) 690-6045.

Notification procedure:

An individual may request information regarding this system of records, or information as to whether this system contains records pertaining to such individual from the System Manager listed above. Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or FSIS Freedom of Information Act (FOIA) Officer, whose contact information can be found at <http://www.da.usda.gov/foia.htm> under "Contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief FOIA Officer, U.S. Department of Agriculture, 1400 Independence Avenue, SW., Washington, D.C. 20250.

When seeking records about yourself from this system of records or any other USDA system of records, your request must conform with the Privacy Act regulations set forth in 7 CFR Part 1. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must

either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief FOIA Officer, U.S. Department of Agriculture, 1400 Independence Avenue, S.W., Washington, D.C. 20250. In addition, you should provide the following:

- An explanation of why you believe USDA would have information on you,
- Which components of USDA you believe may have the information about you,
- When you believe the records would have been created,
- Any other information that will help the FOIA staff determine which USDA component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity.

Records access procedures:

See "Notification Procedure" above.

Contesting records procedures:

See "Notification Procedure" above.

Record source categories:

Information generally is obtained directly from the individual who is the subject of the records, or from someone acting on their behalf, such as Federal, State and Local health agencies, relatives, or a friend of the consumer.

Exemptions claimed for the system:

None

**United States Department of Agriculture
Food Safety and Inspection Service
Consumer Complaint Monitoring System (CCMS) II
FSIS-2011-0030
New System of Records - Narrative Statement**

The mission of the Food Safety and Inspection Service (FSIS) is to protect public health by ensuring that meat, poultry, and processed egg products are safe, wholesome, and accurately labeled. Natural events, accidents, or intentional acts can put the safety of food and the food supply chain at risk, and by doing so, put the health and welfare of consumers at risk. FSIS developed the Consumer Complaint Monitoring System (CCMS II) to help Agency personnel quickly and effectively identify potentially unsafe meat, poultry, or processed egg products. CCMS II is an electronic database accessed from FSIS' Intranet and is used to record, sort, evaluate, and track complaints about possible adverse effects from meat, poultry, or processed egg products regulated by FSIS. CCMS II is also used to track subsequent analysis and investigations of these complaints.

Under the Federal Meat Inspection Act (21 U.S.C. 601, *et seq.*), the Poultry Product Inspection Act (21 U.S.C. 451, *et seq.*), and the Egg Products Inspection Act (21 U.S.C. 1031, *et seq.*), Congress has provided for the inspection and regulated processing and distribution of meat and meat products, poultry, and egg products to prevent the sale and movement in commerce of articles that are adulterated or misbranded. Specifically, 21 U.S.C. 451, 602, and 1031 note that the health and welfare of consumers are to be protected by assuring that meat and meat food products are wholesome and that regulation by the Secretary of Agriculture and cooperation by the States and other jurisdictions are appropriate to protect the health and welfare of consumers.

Further, under 21 U.S.C. 679c (a) (1) and (3), the Secretary is authorized to give high priority to enhancing the ability of FSIS “...to ensure the safety and wholesomeness of meat and poultry products” and to “strengthen the ability of [FSIS] to collaborate with relevant agencies within the Department of Agriculture and with other entities in the Federal Government, the States, and Indian tribes... through the sharing of information and technology.” CCMS II helps to identify products in commerce that are potentially adulterated and enables FSIS to determine whether reported products are safe and wholesome. In addition, the system allows the Agency to collaborate with federal, State, local, and tribal public health partners in identifying potentially unsafe meat or poultry products—and helps the Agency to protect the consuming public from further harm.

A complaint can be initiated by calls from consumers or their representatives, by representatives of State or local health departments and Federal agencies, including USDA’s Agricultural Marketing Service and Food and Nutrition Service, or via electronic hand-off from USDA’s Meat and Poultry Hotline system and through web forms submitted by consumers. The information from these complaints, collected in CCMS II, is analyzed, evaluated, and classified as needing further action by trained analysts in FSIS’ Office of Public Health Science (OPHS). These and other analysts identify the organization that will perform any subsequent action, provide ongoing updates, coordinate communication with other USDA agencies as needed, and alert management in the event of a non-routine incident. OPHS will also determine and coordinate any needed laboratory analysis and provide technical and scientific support to other program areas. Until the complaint is resolved, any action taken is updated in CCMS II.

CCMS II data can include certain information about individuals, such as first and last names, home or work address, telephone number or e-mail, food product consumed, medical symptoms experienced, and medical care received. Some of this information can be and is used to retrieve records, such as first and last name, but by design and in general practice, a system-generated case code is used for retrieval. The case code is sequentially assigned at the time of the initial contact, and is provided to the submitter of the complaint. Other database fields, such as establishment number or type of complaint, can also be used for retrieval.

The data within CCMS II is specifically used for the reasons the information was obtained: to help determine the safety of specific food products consumed by individuals who reported problems with the food items. Information from CCMS II may be shared in a controlled manner within FSIS and, as needed, with other public health partners, to determine whether there is a potential problem with the product, to help identify the origin of the product, to trace forward the product's distribution or disposition, to follow-up with the individual who reported the problem, to ascertain whether others experienced similar problems with the same product, or for other reasons that derive directly from the reason the information was originally collected. There are other routine uses of CCMS II data permitted under U.S.C. 552a (b) (3), as contained in the Federal Register Notice and summarized here:

To the Department of Justice for litigation purposes; to National Archives and Records Administration for records management; to a Congressional Office in response to an inquiry from the relevant constituent; to an appropriate authority for audit purposes; to an appropriate authority in response to a threat to information security or confidentiality; to an appropriate law

enforcement authority in response to investigations, prosecutions, or enforcement actions; to contractors and agents performing a function on behalf of the agency relating to the collection of information to support surveillance, investigations, and facilitation of rapid detection and response to food borne hazards; to appropriate authorities responsible for public health / monitoring illness outbreaks / ensuring safety of the food supply because the data supports public health officials in their ability to identify public health hazards and mitigate their impact through communication and information sharing among public health partners; and to producing establishments in connection with the Agency's investigation of complaint-related information.

CCMS II data and investigations also support other activities, including complaint-related verification of Hazard Analysis and Critical Control Points in producing establishments, analysis of school lunch product manufacturing specifications, and recall coordination for product(s) identified as adulterated or unwholesome.

SAFEGUARDS/SECURITY PROVIDED FOR THIS SYSTEM:

FSIS has taken significant actions to safeguard the identifiable information about an individual in CCMS II and to control access to the system itself. Access to CCMS II is restricted to trained, authorized FSIS employees and to a limited number of users representing FSIS' public health partners in the Department of Health and Human Services. Authorized users are assigned level-of-access roles based on their job functions. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user. Firewalls and other security controls further prevent unauthorized access. As a result, the potential effect of CCMS II on an individual's privacy is minimal.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, records maintained in the system may be disclosed outside USDA for eight routine uses. These routine uses may be described as functional and housekeeping uses.

The records are protected by the confidentiality requirements of USDA's Office of the Chief Information Officer Cyber Security Manuals and the provisions of the Privacy Act. Only authorized USDA employees and contractors will have access to the records in this system, and this access will be on a need-to-know basis. Role-based access controls are used to restrict access to CCMS II, which is accessible via the FSIS Intranet.

The system has been categorized as a Moderate impact system as identified in Federal Information Processing Standard (FIPS) 199. The security controls implemented within the system will correspond with those published in the National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Technology Systems (Revision1) for a Moderate impact system. Users are granted system access only upon successful completion of security training and must successfully complete security training each year to retain access. Each user is supplied with a unique and strong user-id and password. The user roles are restrictive and based on the principle of least privilege allowing for adequate performance of job functions and access to information based on a need to know.

Where appropriate, the system also will adhere to the security controls identified in the Federal

Information Security Control Audit Manual (FISCAM). The mandatory requirements of FIPS 199 and FIPS 200 support the Federal Information Security Management Act and FISCAM supports the mandated Office of Management and Budget Circular A-123, Management of Internal Controls.

Moreover, system managers and users observe and adhere to specific USDA security requirements as set forth in the USDA Cyber Security Manuals, including but not limited to USDA Departmental Manual (DM) 3545-000, Personnel Security, and DM 3510-001, Physical Security Standards for Information Technology Restricted Space.

[FR Doc. 2015-22085 Filed: 9/4/2015 08:45 am; Publication Date: 9/8/2015]